FORM PTO-1390 (REV 10-2000) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: OTV-1021-US

U.S. APPLICATION NO (If known, see 37 CFR 1 5): 09/980271

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/IB99/01213	4 June 1999	4 June 1999

TITLE OF INVENTION: FLEXIBLE INTERFACE FOR SECURE INPUT OF PIN CODE

APPLICANT(S) FOR DO/EO/US: Alain Delpuch

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☑ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S C 371.
3. ☑ This is an express request to promptly begin national examination procedures (35 U S C 371(f))
4. ☐ The US has been elected by the expiration of 19 months from the priority date (PCT Article 31).
5. ☑ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☑ is attached hereto (required only if not communicated by the International Bureau).
   b. ☐ has been communicated by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
7. ☐ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are attached hereto (required only if not communicated by the International Bureau).
   b. ☐ have been communicated by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired
   d. ☐ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☑ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ An English language translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11 to 16 below concern document(s) or information included:

11. ☑ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☐ A FIRST preliminary amendment.
    ☐ A SECOND or SUBSEQUENT preliminary amendment.
14. ☐ A substitute specification.
15. ☑ A change of power of attorney and/or address letter.
16. ☑ Other items or information:

    a) Copy of PCT Request as filed.
    b) Copy of International Search Report
    c) Certificate of Express Mail

U.S. APPLICATION NO (if known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO	ATTORNEY'S DOCKET NUMBER
09/980271	PCT/IB99/01213	OTV-1021-US

17. ☑ The following fees are submitted:

BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :

	CALCULATIONS PTO USE ONLY
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO **$1000.00**	
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO **$860.00**	
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO **$710.00**	
International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) **$690.00**	
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) **$100.00**	
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 740
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	
Total claims	16 - 20 =	0	X $18.00	$ 0
Independent claims	2 - 3 =	0	X $80.00	$ 0
MULTIPLE DEPENDENT CLAIM(S) (if applicable)	3		+ $270.00	$ 840
TOTAL OF ABOVE CALCULATIONS =				$
☐ Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2.				$
SUBTOTAL =				$
Processing fee of **$130.00** for furnishing the English translation later than ☐20 ☐30 months from the earliest claimed priority date (37 CFR 1.492(f)). +				$
TOTAL NATIONAL FEE =				$ 0
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +				$
TOTAL FEES ENCLOSED =				$ 1580
				Amount to be refunded: $
				charged: $

a. ☑ A check in the amount of $ 1580 to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of $_____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☑ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 13-0010 . A duplicate copy of this sheet is enclosed.
(OTV-1021-US)

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

G. Michael Roebuck
Madan, Mossman & Sriram, PC
2603 Augusta, Suite 700
Houston, Texas 77057

G Michael Roebuck
SIGNATURE

G. Michael Roebuck
NAME

35,662
REGISTRATION NUMBER

FLEXIBLE INTERFACE FOR SECURE INPUT OF PIN CODE

The invention is related to interfaces between man and machine such as computer, telephone or television devices, which need a Personal Identification Number (PIN) to authenticate the user running an application.

By running an application, one should understand to continue or to have access to an application or to specific resources of an application.

The invention is more particularly but not exclusively related to a system and a method used in an interactive information system such as an entertainment system.

Requirements for security in interactive entertainment systems are contradictory.

This is because, in order to run an application, an authentication of the user/viewer is needed while using the specific look and feel of the application.

However, it is also preferred that the PIN code should not be given to the application for security purpose.

In fact, two types of solutions are presently known for authentication. Both present drawbacks, as they are only capable of fulfilling part of the above requirements.

Either the application presents its own user interface for PIN entry, then queries the underlying system to check if the given PIN is correct.

This solution does not hide the PIN code from the application.

Or the application requests the underlying system to authenticate the viewer. For this the underlying system, using its own look and feel, prompts the viewer for its PIN, verifies its validity and then returns the information that the viewer is authorised or not to the application.

This solution is safe, but does not allow integration of the PIN entry with the application look and feel.

In other words and referring to figure 1, it is shown a system which presents a good look and feel , but which is not safe, as the PIN code is known by the application.

More precisely, the application 1 has total control of the look and feel.

The viewer provides his PIN code through input means 2 in digital data to the application via an input device, for instance transmitted as infrared signals 3 to the device on which runs the application which displays in 4 the look and feel for the PIN entry field.

Such application, which is now aware of the PIN code, transmits it in 5 to security manager means 6 which, after checking, confirms in 7 authorisation from the system 8.

The PIN code (Input means 2) is therefore provided outside of the system 8, which is unsecured, and may allows third parties to have access to the PIN code.

Figure 2 displays the other way of functioning of a known system of the prior art.

Here, the application 1 has no control over the look and feel, contrarily to the precedent case.

The application 1 requests in 9 the system 8 to identify the user.

The security manager means 6 uses the input means 2 (PIN Code), provided in 3 and the display screen to create in 4 a display of the PIN entry field.

When the security manager means 6 has checked the PIN code, it gives authorisation (7) to display or to access to resource to the application 1.

On a security point of view this system is good as, at no point, the system 8 gives out the PIN code to the application.

However, the look and feel is here totally under system control, without any consideration for the current application look and feel.

It is therefore a main object of the present invention to provide an improved system and method for authorising a secure way of authentication for an access to an application through a PIN code while using the look and feel of said application during the PIN code interrogation.

It is another object of the invention to provide an improved system and method wherein the safety needed for PIN code entry, is combined with perfect integration of the prompt with the service.

It is another objet of the invention to provide a simple and cost saving flexible interface for secure input of a PIN code.

The problems outlined above are in large part solved by a system for authenticating a PIN code of a

user in an interactive information system, in order to run an application which comprises :

- input means for PIN code entry,
- security manager means for comparing the PIN code of the user, upon a request for user authentication from the application, with a registered PIN code, and giving authorisation to run said application if said PIN code of the user matches the registered PIN code,
- and display means for displaying any graphics including a PIN entry field,

characterised in that

the request for user authentication being provided on the display means via the PIN entry field with the look and feel of said application, the system further comprises emitting means for entering crypted digits in said PIN entry field upon entering the PIN code of the user in the security manager means through said input means,

and the security manager means are arranged to give authorisation to run the application after full entry of said crypted digits and if the PIN code of the user is identical to the registered PIN code.

With such system the PIN code remains hidden from the environment, the user having only the impression to enter physically his PIN code within the PIN entry field of the application. In fact, it remains in the security manager means, which is within the system.

In a preferred embodiment the application is a television program.

The invention also provides a method for authenticating a PIN code of a user in an interactive information system, in order to run an application,
wherein said information system emits a request for authenticating a user,
said user enters a PIN code through input means,
said PIN code of the user is compared with a registered PIN code, within security manager means,
and authorisation is provided to run said application if the PIN code of the user matches with the registered PIN code,
characterised in that
- the request for authenticating being provided with a PIN entry field having the look and feel of the application,
- crypted digits are entered in said PIN entry field, upon entering the PIN code by the user in the security manager means,
and authorisation to display the application is only provided after full entry of said crypted digits, and if the PIN code signal of the user is identical to the registered PIN code as checked by the security manager means.

The invention will be better understood from reading the following description of a particular embodiment given by way of non limiting example, and which refers, additionally to the above mentioned figures showing the prior art, to the accompanying drawings in which :

- Figures 1 and 2, already mentioned, are schematic drawings figuring the architecture of the PIN code interface of the prior art.

- Figure 3 is a schematic drawing showing the architecture of the system according to the present invention.

- Figure 4 is a schematic drawing showing an interactive television system for implementing the invention.

- Figure 5 is a flowchart related to the application according to the embodiment of the invention more particularly described here.

- Figure 6 is a flowchart implemented by the security manager means according to the embodiment of the invention more particularly described here.

Figure 3 shows a system 10 arranged to authenticate the user before running an application 11, according to the invention.

The application 11 initiates a PIN entry request 12 to authenticate the user request and simultaneously asks the security manager means 13 to handle key input 14 to be introduced through Input means 15, for instance through a key pad.

The security manager means 13 comprises a small computer system including a central processing unit (CPU), memory and local storage. It is connected to input/output ports.

It is programmed in order to provide the different steps according to the method of the invention.

The application having total control over the graphics displayed and their look and feel, the look

and feel 16 for PIN entry is provided on display means 17 according to the application.

The display means can be a TV screen, an LCD screen of a remote portable telephone, etc.

As the security manager means 13 is asked to enter the PIN entry mode, it grabs key inputs 14, analyses these inputs for user authentication and relays in 18 the key presses to the application.

The security manager means does not relay the key values, which therefore remains within the system, but only relays the fact that a key has been pressed, letting for instance the application display an X for each key pressed, in the PIN entry field.

This way the application does not learn about the PIN, but can give user feedback 19 to the display means 17.

When the security manager means 13 recognises the PIN, it informs in 20 the application that the user/viewer has been authenticated.

The application can then run, be displayed and/or operate.

Figure 4 shows schematically an interactive television system 21 including a system S according to the embodiment of the invention more particularly described here.

A broadcaster 22 transmit through a satellite 23 the signal corresponding to the look and feel of an application request (arrows 24), for instance a Pay TV program.

The signal is provided to a digital interactive decoder 25, currently packaged in a set-top connected to a television 26.

It delivers true interactive television using the broadcast-oriented infrastructure currently predominant in the television industry.

The decoder 25 comprises in a manner known per se, a demultiplexer 27 and an application programming interface 28, stored in a local memory (RAM, EPROM FLASH memory, ...), such as the one proposed by the applicant OPEN TV, and which provides a library of functions which can display graphics on the television screen, control audio/video services, accept user input and communicate with the outside world.

The decoder 25 also comprises a CPU 29, Audio/Video decoding means 30, connected through audio video output 31 to the television set 26, storage means 32 for storing an operating system for the CPU 29, such as the one provided by OPEN TV.

The CPU 29 further includes part of the security manager means 33 as described in the invention.

The decoder 25 also comprises Input means 34 such as infrared sensors arranged to receive infrared signals 35 emitted by a remote control apparatus 36 having a key pad 37, and display function means 38 controlled by the CPU.

The decoder 25 also comprises output means having a modem and/or a multiplexer 39 for providing back return signals 40 on a return channel to the broadcaster 22 and/or a server.

The broadcast system may be, of course based on satellite or cable or some other medium.

Figure 5 shows a block diagram according to an embodiment of the invention to be included in an application to authenticate the users to continue or to have access to specific resources which needs authentication by a PIN code.

The application first uses some display function (block 41) to present a PIN entry field to the viewer.

It then asks the security manager means to enter the PIN entry mode and check in 43 if keys are pressed.

As keys are pressed, it gives (block 44) feedback using the display function.

If the user is not authenticated (step 45), it comes back (loop 46) to check 43.

If the user is authenticated (in 47), there is an OK from the security manager means and the application can go on (step 48).

An example of a block diagram of the security manager program is provided on figure 6 and is performed entirely (and secretly) within the System S.

At the application request in 49, the security manager means enters a PIN entry mode (step 50).

The PIN repertory is then initialised to empty in 51 and the system wait for a key to be pressed (check 52).

If the key is an « ending » key (for instance OK or enter), (check 53) there is a release of the key input grabbing (step 54).

If not there is a loop 55 for more key.

After release of the key input grabbing, the security manager means checks in 56 the entered PIN against the user's PIN.

It then either returns success (step 57), or failure (step 58) to application (step 45 of the application), before exiting PIN entry mode in 59.

It will now be described the functioning of the system while referring to figure 4.

At the broadcast site, pay TV programs of a Specific Provider are stored.

The pay TV programs are encoded into a digital bitstream which is compressed and multiplexed with the signal of the PIN code field of the Specific Provider, including its logo and a menu to allow the viewer to have access to other movies of the provider, to form a single bitstream.

This single bitstream is then broadcasted to all subscribers. At each customer's site, the bitstream is received by the decoder 25 where the audio and video are decompressed and the PIN code field is sent to the customer's television set 26.

The request for the PIN code of the user is therefore prompted to the viewer.

The viewer then, for instance through a remote control apparatus, can enter his PIN code by pressing keys.

At each pressing, a cross appears in the PIN entry field on the TV Screen.

Meanwhile the Security manager means 33 compares the PIN code with a preregistered user's PIN code entered before in the decoder for instance via a modem.

If the PIN codes matches, signals are sent to the application decoding process 30, and such decoding process is then authorised for displaying the application on the TV set.

Additional advantages and modifications will readily occur to those skilled in the art. Therefore the present invention in its broader aspects is not limited to the specific details, representative devices and illustrated examples shown and described herein.

For instance, it also includes application to PIN code entry for obtaining specific services through mobile phone, for instance via GSM, or other specific services via Television and/or Internet.

CLAIMS

1. A system (10, S) for authenticating a PIN code of a user in an interactive information system in order to run an application (11),

wherein it comprises

- input means (15, 34, 35, 36, 37) for PIN code entry,

- security manager means (13, 33) for comparing the PIN code of the user upon a request for user authentication from the application, with a registered PIN code, and giving authorisation to run said application if the PIN code of the user matches with the registered PIN code, and

- display means (17, 29, 38) for displaying any graphics including a PIN entry field,

characterised in that

the request for user authentication being provided on the display means via the Pin entry field with the look and feel of said application, the system further comprises emitting means (29, 38) for entering crypted digits in said PIN entry field upon entering the PIN code of the user in the security manager means through said input means,

and the security manager means (13, 33) are arranged to give authorisation to run the application after full entry of said crypted digits and if the PIN code of the user is identical to the registered PIN code.

2. A system according to claim 1 characterised in that the application is a television program.

3. A system according to claim 1, characterised in that the application is a service provided on mobile Telephone.

4. A method for authenticating a PIN code of a user in an interactive information system, in order to run an application,

wherein said information system emits a request for authenticating a user (41),

said user enters a PIN code (43) through input means,

said PIN code of the user is compared (45) with a registered PIN code within security manager means,

and authorisation is provided to run said application if the PIN code of the user matches with the registered PIN code,

characterised in that

- the request for authenticating being provided with a PIN entry field having the look and feel of the application,
- crypted digits are entered (44) in said PIN entry field, upon entering the PIN code by the user in the security manager means,

and authorisation to display the application is only provided (47) after full entry of said crypted digits, and if the PIN code of the user is identical to the registered PIN code as checked by the security manager means.

5. A method according to claim 4, characterised in that, for presenting the request for authentication, the application undertakes the following steps :

- presenting a PIN entry field to the user (41),
- asking the security manager means to enter a PIN Entry Mode (42),
- the input means comprising keys, checking if keys are pressed by the user (43),
- while keys are pressed, giving feedback in entering said crypted digits in said PIN entry field (44), and,
- if the user is authenticated (45) by said security manager means, giving said authorisation (47) to display (48) the application.

6. A method according to any of claims 4 and 5, characterised in that, for providing the authorisation to display the application the security manager means undertakes the following steps :
- at the request of the application entering a PIN entry mode (50),
- initialising to empty a PIN repertory (51) and, the input means comprising keys, waiting for a key to be pressed by the user (52),
- upon occurrence of pressing an « ending key », checking if a release occurs (53), checking the entered PIN against the user's PIN (56), and if success authorising the application to run.

7. A method according to any of claims 4 to 6, characterised in that the application is a Television program.

8. A method according to any of claims 4 to 6, characterised in that the application is a service provided on a mobile telephone.

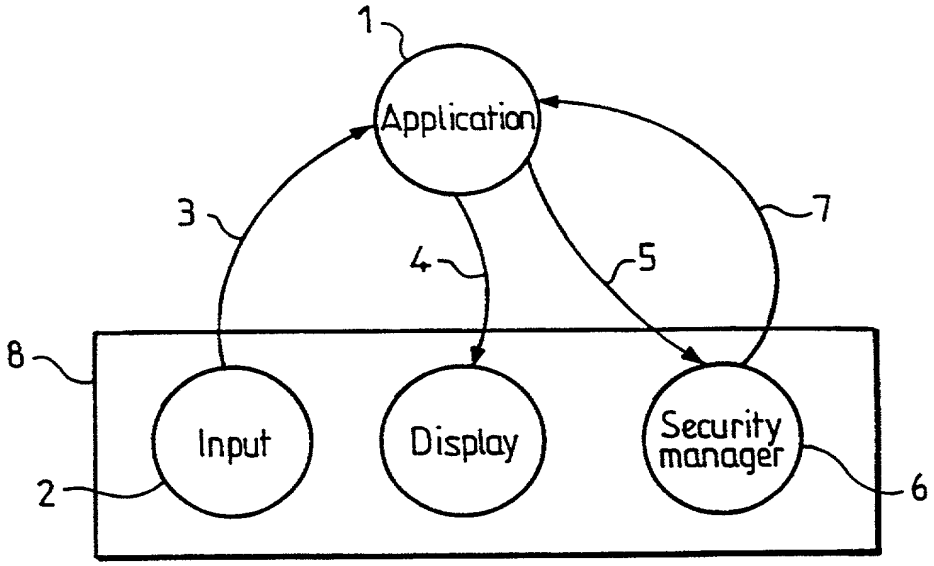

FIG.1 PRIOR ART

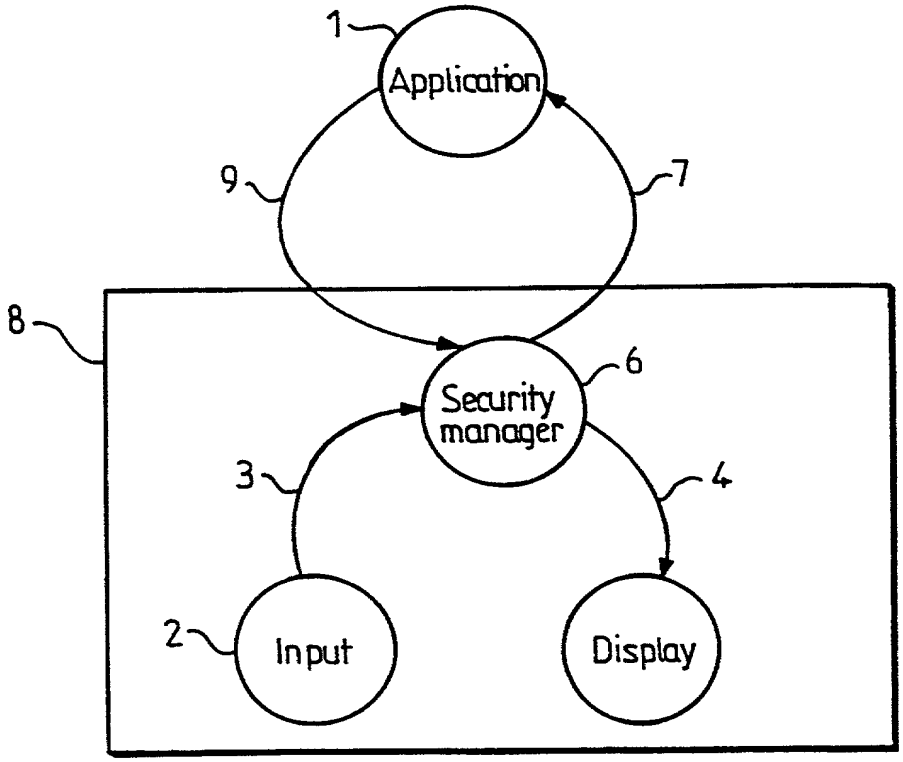

FIG.2 PRIOR ART

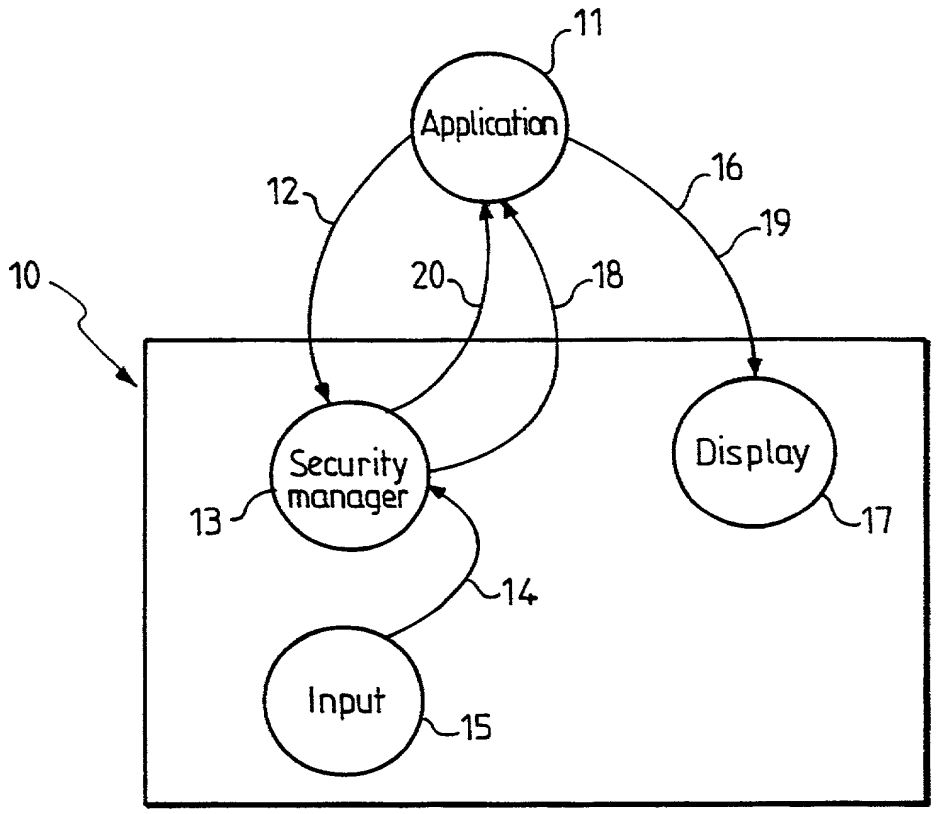
11
Application
12
16
19
10
20
18
Security manager
13
Display
17
14
Input
15

FIG. 3

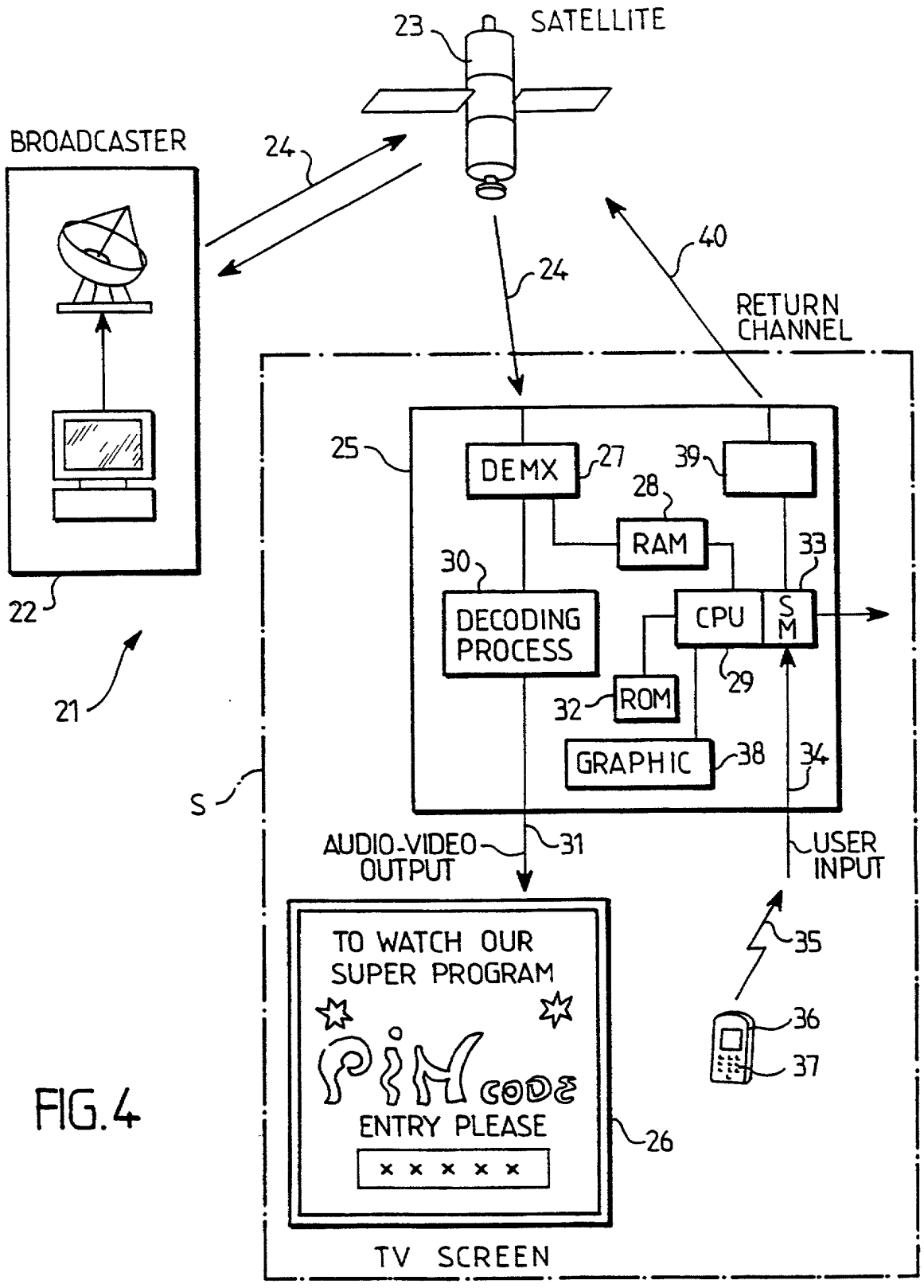
SATELLITE
23
BROADCASTER
24
24
40
RETURN CHANNEL
25
DEMX
27
39
28
RAM
33
30
DECODING PROCESS
CPU
S M
29
32
ROM
GRAPHIC
38
34
22
21
S
AUDIO-VIDEO OUTPUT
31
USER INPUT
TO WATCH OUR SUPER PROGRAM
PIN CODE
ENTRY PLEASE
× × × × ×
26
35
36
37
TV SCREEN

FIG.4

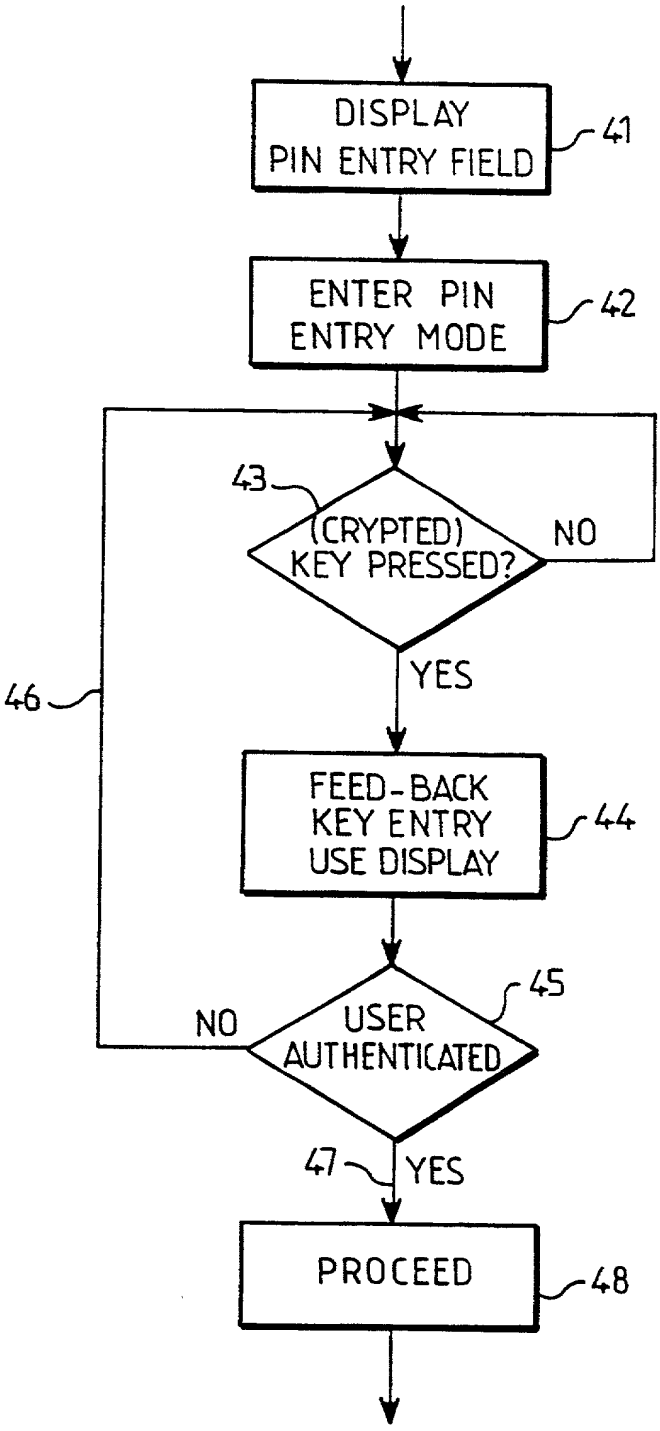
DISPLAY PIN ENTRY FIELD
41
ENTER PIN ENTRY MODE
42
43
(CRYPTED) KEY PRESSED?
NO
YES
46
FEED-BACK KEY ENTRY USE DISPLAY
44
45
NO
USER AUTHENTICATED
47
YES
PROCEED
48

FIG.5

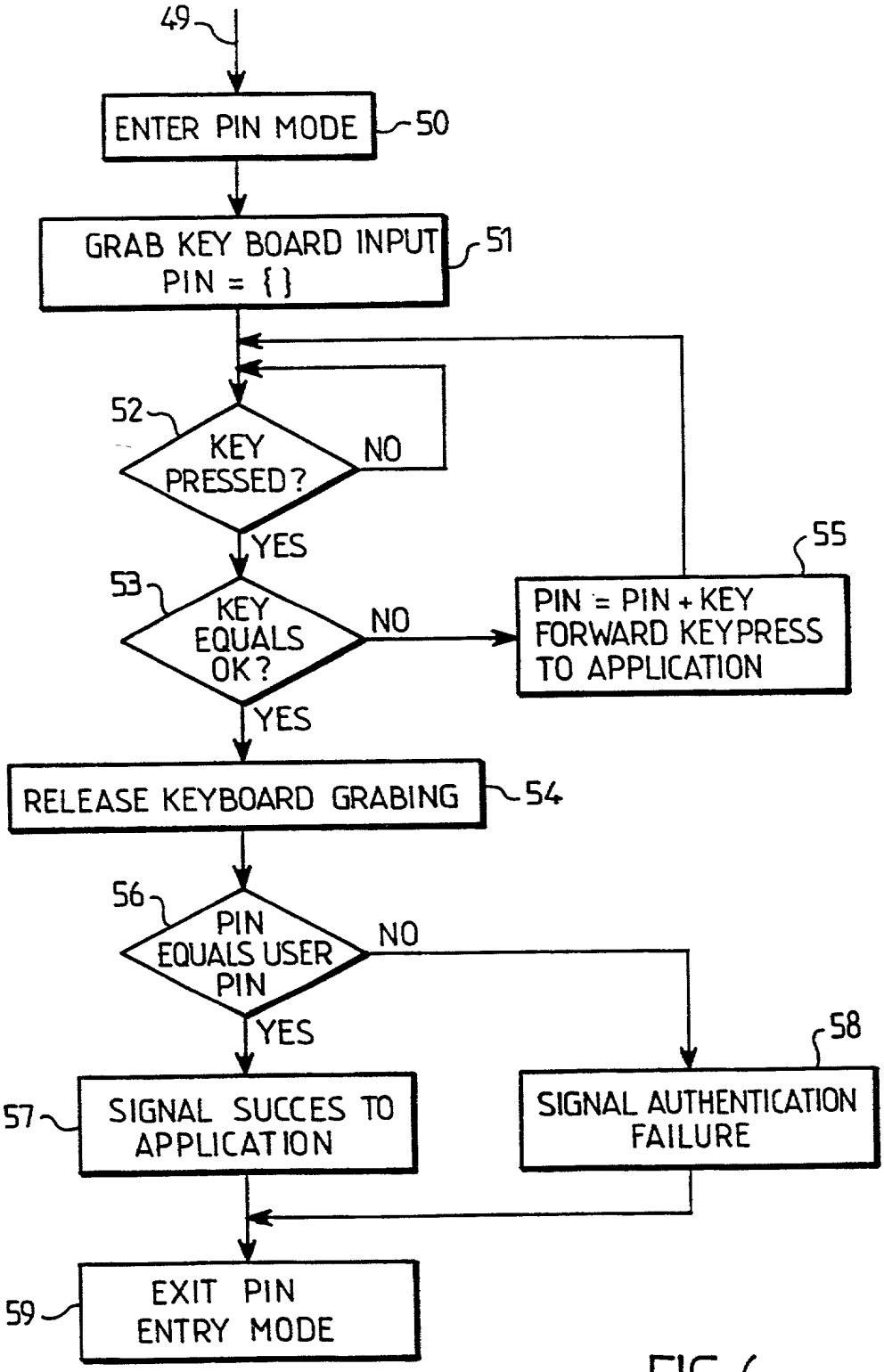
49
ENTER PIN MODE
50
GRAB KEY BOARD INPUT
PIN = { }
51
52
KEY PRESSED?
NO
YES
53
KEY EQUALS OK?
NO
55
PIN = PIN + KEY
FORWARD KEYPRESS
TO APPLICATION
YES
RELEASE KEYBOARD GRABING
54
56
PIN EQUALS USER PIN
NO
YES
58
57
SIGNAL SUCCES TO APPLICATION
SIGNAL AUTHENTICATION FAILURE
59
EXIT PIN ENTRY MODE

FIG.6

DECLARATION FOR PATENT APPLICATION

As the below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below under my name.

I believe that I am the original, first inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled **"Flexible Interface for Secure Input of PIN Code"**, the specification of which is filed concurrently.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose all information known to me, which is material to patentability as defined in Title 37, Code of Federal Regulations, Sec. 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Sec. 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed.

PRIOR FOREIGN APPLICATION(S)

NUMBER	COUNTRY	(DAY/MONTH/YEAR FILED)	PRIORITY CLAIMED
PCT/IB99/01213	PCT	4 June 1999	YES X NO

I hereby claim the benefit under Title 35, United States Code, Sec. 120 of any United States application listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in any prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Sec. 112, I acknowledge the duty to disclose information which is material to patentability as defined by Title 37, Code of Federal Regulations, Sec. 1.56, which became available between the filing date of the prior application and the national or PCT international filing date of this application:

SERIAL NO.	FILING DATE	STATUS

Please address all correspondence regarding this application to:

G. Michael Roebuck
Madan, Mossman & Sriram P.C.
2603 Augusta Drive, Suite 700
Houston, Texas 77057
Telephone: 713/266-1130
Facsimile: 713/266-8510

Direct all telephone calls to **G. Michael Roebuck** at (713) 266-1130, ext. 105.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Sec. 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Inventor: 1-00 Alain Delpuch

Residence: 20 Ave. Andre Prothin, 92927 Paris La Defense cedex

Post Office Address: 20 Ave. Andre Prothin, 92927 Paris La Defense cedex

Citizen Of: France FRX

Date: Oct 25 2001

Signature: